UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS
EASTERN DIVISION

JAMES LACKNER, on behalf of himself and all others similarly situated, Plaintiff, v. **SENSATA TECHNOLOGIES, INC.**, Defendant.	Case No. **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiff, James Lackner ("Plaintiff"), individually and on behalf of all others similarly situated, complains and alleges as follows against Defendant, Sensata Technologies, Inc. ("Defendant" or "Sensata") based on personal knowledge, on the investigation of his counsel, and on information and belief as to all other matters:

INTRODUCTION

1. This is a civil action seeking monetary damages and injunctive and declaratory relief from Defendant Sensata, arising from its failure to safeguard certain Personally Identifying Information ("PII") and protected health information ("PHI") (collectively "Private Information") of thousands of its current and former employees and employees' dependents, resulting in Defendant's network systems being unauthorizedly accessed between March 28, 2025, and April 6, 2025.

2. According to Defendant's Breach Notice, on or around April 6, 2025, Sensata "determined that certain servers in our network were encrypted with ransomware." A copy of Plaintiff's Breach Notice is attached as Exhibit A.

3. Worse, an internal investigation revealed that "an unauthorized actor viewed and

obtained files" from Defendant's network. Ex. A.

4. Upon information and belief, the total number of individuals who have had their data exposed due to Defendant's failure to implement appropriate security safeguards is approximately 15,630.[1]

5. On information and belief, cybercriminals were able to breach Defendant's systems because Defendant failed to adequately train its employees on cybersecurity and failed to maintain reasonable security safeguards or protocols to protect the Class's Private Information. In short, Defendant's failures placed the Class's Private Information in a vulnerable position—rendering them easy targets for cybercriminals.

6. On or around June 5, 2025–more than *two months* after the Data Breach first occurred–Sensata finally began notifying Class Members about the Data Breach ("Breach Notice").

7. Plaintiff is a Data Breach victim. He brings this class action on behalf of himself, and all others harmed by Defendant's misconduct.

8. The exposure of one's Private Information to cybercriminals is a bell that cannot be unrung. Before this data breach, its current and former employees' and their dependents' Private Information was exactly that—private. Not anymore. Now, their PII is forever exposed and unsecure.

PARTIES

9. Plaintiff James Lackner is a natural person and citizen of the state of Arizona, residing in Cave Creek, Arizona.

10. Defendant, Sensata Technologies, Inc. is a foreign corporation organized and

[1] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed November 21, 2024).

existing under the laws of the state of Delaware, with a principal place of business at 529 Pleasant Street, Attleboro, MA 02703.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. There are over 100 Putative Class Members.

12. This Court has personal jurisdiction over Defendant because it is headquartered in Massachusetts and regularly conducts business in Massachusetts. Defendant and Plaintiff are citizens of different states.

13. Venue is proper in this Court under because Defendant's principal office is in this District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

Sensata Technologies

14. Sensata is a "global industrial technology company" with over "18,000 companies and operations in 14 countries."[2]

15. On information and belief, Sensata failed to undertake adequate measures to safeguard the Private Information of Plaintiff and the proposed Class Members, including failing to implement industry standards for data security, and failing to properly train employees on cybersecurity protocols, resulting in the Data Breach.

[2] https://www.sensata.com/about (last accessed November 21, 2024).

16. In collecting and maintaining the Private Information, Defendant agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiff and Class members themselves took reasonable steps to secure their Private Information.

17. Under state and federal law, businesses like Defendant have duties to protect their current and former employees' and their dependents' Private Information and to notify them about breaches.

18. Defendant recognizes these duties, declaring in its "Privacy Policy:"

a. "Sensata Technologies is committed to respecting your privacy;"

b. "We retain your information for as long as is necessary to accomplish the purpose for which it was collected;"

c. "We implement a range of technical and organizational measures designed to provide a level of security appropriate to the risk to the personal information we process, including to address the on-going integrity, confidentiality, and availability of personal information;" and

d. "We evaluate these measures on a regular basis."[3]

19. As a direct and proximate result of Defendant's failures to protect Plaintiff's and the Class Members' sensitive personal information and warn them promptly and fully about the Data Breach, Plaintiff and the proposed Class have suffered widespread injury and damages necessitating Plaintiff seeking relief on a class wide basis.

Plaintiff and the Class Members entrusted their Private Information to Sensata

20. Plaintiff and the Class are current and former Sensata employees and their dependents.

[3] https://www.sensata.com/resources/privacy-policy (last visited June 12, 2025).

21. As a condition of employment with Sensata, Plaintiff and the Class Members were required by Sensata to provide their sensitive and confidential Private Information, including, but not limited to, their Social Security number, tax identification number, driver's license number or state-issued identification card number, passport number, other government-issued identification number, financial account information, payment card information, medical information, health insurance information, and/or date of birth. Ex. A.

22. Sensata maintains records of its employees' and their dependents' information such as their Social Security number, tax identification number, driver's license number or state-issued identification card number, passport number, other government-issued identification number, financial account information, payment card information, medical information, health insurance information, and/or date of birth in the ordinary course of business. These records are stored on Sensata's network systems.

23. Upon information and belief, Defendant maintains employee information long after the employment relationship has been terminated.

24. Sensata acquired, collected, and stored a massive amount of said Private Information of its employees, including Plaintiff and the Members of the proposed Class, which it stored in its electronic systems.

25. By obtaining, collecting, using, and deriving a benefit from its employees' and their dependents' Private Information, Sensata assumed legal and equitable duties to those individuals and knew or should have known that it was responsible for protecting their Private Information from unauthorized disclosure.

26. Plaintiff has taken reasonable steps to maintain the confidentiality of his Private Information. Plaintiff, as a former employee, relied on Sensata to keep his Private Information

confidential and securely maintained, to use this information for authorized purposes and disclosures only.

27. Plaintiff and the proposed Class Members entrusted their Private Information to Sensata solely for the purposes of applying for employment with Defendant and/or as a condition of employment, with the expectation and implied mutual understanding that Sensata would strictly maintain the confidentiality of the information and undertake adequate measures to safeguard it from theft or misuse.

28. Plaintiff and the proposed Class Members would not have entrusted Sensata with their highly sensitive Private Information if they had known that Sensata would fail to take adequate measures to protect it from unauthorized use or disclosure.

Plaintiff's and the Class Members' Private Information was Improperly Disclosed and Compromised in the Data Breach

29. As a prerequisite to employment, Plaintiff and the Class Members disclosed their non-public and sensitive Private Information to Sensata, with the implicit understanding that their Private Information would be kept confidential. This understanding was based on all the facts and circumstances attendant to their employment there, and the express, specific, written representations made by Sensata and its agents.

30. Plaintiff and the Class Members reasonably relied upon Sensata's representations to their detriment and would not have provided their sensitive Private Information to Sensata if not for Sensata's explicit and implicit promises to adequately safeguard that information.

31. On April 6, 2025, Sensata "determined that certain servers in [its] network were encrypted with ransomware." Ex. A.

32. An internal investigation revealed that cybercriminals had accessed its systems between March 28, 2025, and April 6, 2025, giving cybercriminals unfettered access to its system

for an entire ***ten days***. Ex. A.

33. Worryingly, Defendant admitted that the unauthorized actor had not only accessed its system, but also *exfiltrated* certain files from the system, stating that "an unauthorized actor viewed and **obtained** files from our network." Ex. A.

34. Additionally, on April 6, 2025, Sensata filed an 8-K SEC form announcing that it had experienced a cybersecurity incident in which there was "evidence that files were taken from the Company's environment."[4] Further, Defendant admitted "the full scope and impact of this incident is not yet known."[5]

35. Despite this, Defendant waited until June 5, 2025—almost *two months* after the Data Breach began—to begin notifying victims that their Private Information had been compromised and stolen during the Data Breach. *See* Exhibit A.

36. Defendant represented in its Breach Notice that it has "taken additional steps to enhance our existing security measures." Ex. A. However, this is too little too late because these steps should have been taken *before* the Data Breach.

37. Sensata's Breach Noticed acknowledged the increased risk faced by victims of the Data Breach when it urged those affected to sign up for credit monitoring services to "detect potential misuse of your information and offers identity protection solutions aimed at promptly identifying and resolving any instances of identity theft." Ex. A.

38. Although Sensata offered several months of complimentary credit monitoring, this is insufficient to address the lifelong risk that victims now face due to the Data Breach.

39. As a result of this Data Breach, the Private Information of Plaintiff and the proposed

---

[4]https://www.sec.gov/ix?doc=/Archives/edgar/data/0001477294/000147729425000047/st-20250406.htm (last accessed November 22, 2024).

[5] *Id.*

Class Members was unauthorizedly disclosed and compromised in the Data Breach.

40. The Data Breach was preventable and a direct result of Sensata's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect employees' and their dependents' Private Information.

41. Worryingly, Defendant admits that the Data Breach was the result of a ransomware attack in which its systems were encrypted, meaning that cybercriminals now have access to victims Private Information. Ex. A.

42. And as the Harvard Business Review notes, such "[c]ybercriminals frequently use the Dark Web—a hub of criminal and illicit activity—to sell data from companies that they have gained unauthorized access to through credential stuffing attacks, phishing attacks, [or] hacking."[6]

43. Thus, on information and belief, Plaintiff's and the Class's stolen Private Information has already been published—or will be published imminently—by cybercriminals on the Dark Web.

Plaintiff's Experiences and Injuries

44. Plaintiff James Lackner is a former employee of Defendant.

45. As a condition of employment, Defendant required Plaintiff to provide it with his Private Information. Defendant thus obtained and maintained Plaintiff's Private Information.

46. Plaintiff provided his Private Information to Defendant and trusted that the company would use reasonable measures to protect it according to Sensata's internal policies as well as state and federal law.

47. As a result, Plaintiff was injured by Defendant's Data Breach.

---

[6] Brenda R. Sharton, *Your Company's Data Is for Sale on the Dark Web. Should You Buy It Back?*, HARVARD BUS. REV. (Jan. 4, 2023) https://hbr.org/2023/01/your-companys-data-is-for-sale-on-the-dark-web-should-you-buy-it-back.

48. Upon information and belief, Defendant maintained Plaintiff's Private Information long after the employment relationship had ended.

49. Plaintiff received a Notice of Data Breach in June 2025.

50. Through its Data Breach, Defendant compromised Plaintiff's Private Information including his Social Security number, tax identification number, driver's license number or state-issued identification card number, passport number, other government-issued identification number, financial account information, payment card information, medical information, health insurance information, and/or date of birth. Ex. A.

51. On information and belief, Plaintiff's Private Information was obtained by cybercriminals and has been, or will be, published on the dark web.

52. Plaintiff has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. After all, Defendant directed Plaintiff to take those steps in its breach notice. *See* Ex. A.

53. Plaintiff fears for his personal financial security and worries about what information was exposed in the Data Breach.

54. Because of Defendant's Data Breach, Plaintiff has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

55. Plaintiff suffered actual injury from the exposure and theft of his Private Information— which violates his rights to privacy.

56. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his Private Information. After all, Private Information is a form of intangible property—

property that Defendant was required to adequately protect.

57. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff's Private Information right in the hands of criminals.

58. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of time and money to try and mitigate his injuries.

59. Today, Plaintiff has a continuing interest in ensuring that his Private Information— which, upon information and belief, remains backed up in Defendant's possession— is protected and safeguarded from additional breaches.

Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

60. Because of Defendant's failure to prevent the Data Breach, Plaintiff and Class members suffered—and will continue to suffer—damages. These damages include, *inter alia*, monetary losses, lost time, anxiety, and emotional distress. Also, they suffered or are at an increased risk of suffering:

a. loss of the opportunity to control how their Private Information is used.

b. diminution in value of their Private Information.

c. compromise and continuing publication of their Private Information.

d. out-of-pocket costs from trying to prevent, detect, and recovery from identity theft and fraud.

e. lost opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, *inter alia*, preventing, detecting, contesting, and recovering from identify theft and fraud.

f. delay in receipt of tax refund monies.

g. unauthorized use of their stolen Private Information; and

h. continued risk to their Private Information—which remains in Defendant's possession—and is thus as risk for futures breaches so long as Defendant fails to take appropriate measures to protect the Private Information.

61. Stolen Private Information is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen Private Information can be worth up to $1,000.00 depending on the type of information obtained.

62. The value of Plaintiff and Class's Private Information on the black market is considerable. Stolen Private Information trades on the black market for years. And criminals frequently post and sell stolen information openly and directly on the "dark web"— further exposing the information.

63. It can take victims years to discover such identity theft and fraud. This gives criminals plenty of time to sell the Private Information far and wide.

64. One way that criminal's profit from stolen Private Information is by creating comprehensive dossiers on individuals called "Fullz" packages. These dossiers are both shockingly accurate and comprehensive. Criminals create them by cross- referencing and combining two sources of data, first the stolen Private Information, and second, unregulated data found elsewhere on the internet (like phone numbers, emails, addresses, etc.).

65. The development of "Fullz" packages means that the Private Information exposed in the Data Breach can easily be linked to data of Plaintiff and the Class that is available on the internet.

66. In other words, even if certain information such as emails, phone numbers, or

credit card numbers may not be included in the Private Information stolen by the cyber- criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and Class members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other Class members' stolen Private Information is being misused, and that such misuse is fairly traceable to the Data Breach.

67. Defendant disclosed the Private Information of Plaintiff and Class members for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the Private Information of Plaintiff and Class members to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen Private Information.

68. Defendant's failure to promptly and properly notify Plaintiff and Class members of the Data Breach exacerbated Plaintiff and Class members' injury by depriving them of the earliest ability to take appropriate measures to protect their Private Information and take other necessary steps to mitigate the harm caused by the Data Breach.

Consumers Prioritize Data Security

69. In 2024, the technology and communications conglomerate Cisco published the results of its multi-year "Consumer Privacy Survey."[7] Therein, Cisco reported the following:

a. "For the past six years, Cisco has been tracking consumer trends across the privacy landscape. During this period, privacy has evolved from relative

[7] *Privacy Awareness: Consumers Taking Charge to Protect Personal*, CISCO, https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-report-2024.pdf (last visited March 19, 2025).

obscurity to a customer requirement with more than 75% of consumer respondents saying they won't purchase from an organization they don't trust with their data."[8]

b. "Privacy has become a critical element and enabler of customer trust, with 94% of organizations saying their customers would not buy from them if they did not protect data properly."[9]

c. 89% of consumers stated that "I care about data privacy."[10]

d. 83% of consumers declared that "I am willing to spend time and money to protect data" and that "I expect to pay more" for privacy.[11]

e. 51% of consumers revealed that "I have switched companies or providers over their data policies or data-sharing practices."[12]

f. 75% of consumers stated that "I will not purchase from organizations I don't trust with my data."[13]

Defendant Knew—Or Should Have Known—of the Risk of a Data Breach

70. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in recent years.

71. According to the *2023 Annual Data Breach Report*, the number of data compromises in 2023 nearly doubled compared to 2022.[14] And in 2023, a record 3,205 breaches

[8] *Id*. at 3.
[9] *Id*.
[10] *Id*. at 9.
[11] *Id*.
[12] *Id*.
[13] *Id*. at 11.
[14] https://www.idtheftcenter.org/post/2023-annual-data-breach-report-reveals-record-number-of-compromises-72-percent-increase-over-previous-high/ (last visited November 21, 2024).

occurred, exposing the data of approximately 353,027,892 victims.[15]

72. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service issue warnings to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[16]

73. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

Defendant Failed to Follow FTC Guidelines

74. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. Thus, the FTC issued numerous guidelines identifying best data security practices that businesses—like Defendant—should use to protect against unlawful data exposure.

75. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*. There, the FTC set guidelines for what data security principles and practices businesses must use.[17] The FTC declared that, *inter alia*, businesses must:

a. protect the personal customer information that they keep.

b. properly dispose of personal information that is no longer needed.

---

[15] *Id.*

[16] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.

[17] *Protecting Personal Information: A Guide for Business,* FEDERAL TRADE COMMISSION (Oct. 2016) https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

c. encrypt information stored on computer networks.

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

76. The guidelines also recommend that businesses watch for the transmission of large amounts of data out of the system—and then have a response plan ready for such a breach.

77. Furthermore, the FTC explains that companies must:

a. not maintain information longer than is needed to authorize a transaction.

b. limit access to sensitive data.

c. require complex passwords to be used on networks.

d. use industry-tested methods for security.

e. monitor for suspicious activity on the network; and

f. verify that third-party service providers use reasonable security measures.

78. The FTC brings enforcement actions against businesses for failing to protect customer data adequately and reasonably. Thus, the FTC treats the failure— to use reasonable and appropriate measures to protect against unauthorized access to confidential consumer data—as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

79. In short, Defendant's failure to use reasonable and appropriate measures to protect against unauthorized access to employees' and their dependents' data constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Failed to Follow Industry Standards

80. Several best practices have been identified that—at a *minimum*— should be implemented by businesses like Defendant. These industry standards include educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption (making data unreadable without a key); multi-factor authentication; backup data; and limiting which employees can access sensitive data.

81. Other best industry standard practices include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

82. Upon information and belief, Defendant failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04).

83. These frameworks are applicable and accept industry standards. And by failing to comply with these accepted standards, Defendant opened the door to the criminals—thereby causing the Data Breach.

CLASS ACTION ALLEGATIONS

84. Plaintiff brings this class action under Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of all members of the following class:

All individuals residing in the United States whose Private Information was

compromised in the Sensata the Data Breach, including all those individuals who received notice of the breach.

85. Excluded from the Class are Sensata and its subsidiaries and affiliates, officers, directors, and members of their immediate families, and any entity in which it has a controlling interest, the legal representatives, heirs, successors or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

86. Plaintiff reserves the right to amend the class definition.

87. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of her claims on class-wide basis using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

88. Ascertain ability. All members of the proposed Class are readily ascertainable from information in Defendant's custody and control. After all, Defendant already identified some individuals and sent them data breach notices.

89. Numerosity. The Class members are so numerous that joinder of all Class members is impracticable. Upon information and belief, the proposed Class includes at least 15,630 members.

90. Typicality. Plaintiff's claims are typical of Class members' claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

91. Adequacy. Plaintiff will fairly and adequately protect the proposed Class's common interests. His interests do not conflict with Class members' interests. And Plaintiff has retained counsel—including lead counsel—that is experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf.

92. Commonality and Predominance. Plaintiff's and the Class's claims raise predominantly common fact and legal questions—which predominate over any questions affecting individual Class members—for which a class wide proceeding can answer for all Class members. In fact, a class wide proceeding is necessary to answer the following questions:

a. if Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's PII.

b. if Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach.

c. if Defendant were negligent in maintaining, protecting, and securing PII.

d. if Defendant breached contract promises to safeguard Plaintiff and the Class's PII.

e. if Defendant took reasonable measures to determine the extent of the Data Breach after discovering it.

f. if Defendant's Breach Notice was reasonable.

g. if the Data Breach caused Plaintiff and the Class injuries.

h. what the proper damages measure is; and

i. if Plaintiff and the Class are entitled to damages, treble damages, and or injunctive relief.

93. Superiority. A class action will provide substantial benefits and is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class members are relatively small compared to the burden and expense that individual litigation against Defendant would require. Thus, it would

be practically impossible for Class members, on an individual basis, to obtain effective redress for their injuries. Not only would individualize litigation increase the delay and expense to all parties and the courts, but individualized litigation would also create the danger of inconsistent or contradictory judgments arising from the same set of facts. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, ensures economies of scale, provides comprehensive supervision by a single court, and presents no unusual management difficulties.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiff and the Class)

94. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

95. Plaintiff and the Class entrusted their Private Information to Defendant on the premise and with the understanding that Defendant would safeguard their Private Information, use their Private Information for business purposes only, and/or not disclose their Private Information to unauthorized third parties.

96. Defendant owed a duty of care to Plaintiff and Class members because it was foreseeable that Defendant's failure—to use adequate data security in accordance with industry standards for data security—would compromise their Private Information in a data breach. And here, that foreseeable danger came to pass.

97. Defendant has full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and the Class could and would suffer if their Private Information was wrongfully disclosed.

98. Defendant owed these duties to Plaintiff and Class members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew

or should have known would suffer injury-in-fact from Defendant's inadequate security practices. After all, Defendant actively sought and obtained Plaintiff and Class members' Private Information.

99. Defendant owed—to Plaintiff and Class members—at least the following duties to:

a. exercise reasonable care in handling and using the Private Information in its care and custody.

b. implement industry-standard security procedures sufficient to reasonably protect the information from a data breach, theft, and unauthorized.

c. promptly detect attempts at unauthorized access.

d. notify Plaintiff and Class members within a reasonable timeframe of any breach to the security of their Private Information.

100. Thus, Defendant owed a duty to timely and accurately disclose to Plaintiff and Class members the scope, nature, and occurrence of the Data Breach. After all, this duty is required and necessary for Plaintiff and Class members to take appropriate measures to protect their Private Information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

101. Defendant also had a duty to exercise appropriate clearinghouse practices to remove Private Information it was no longer required to retain under applicable regulations.

102. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the Private Information of Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

103. Defendant's duty to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential Private Information, a necessary part of obtaining employment from Defendant.

104. The risk that unauthorized persons would attempt to gain access to the Private Information and misuse it was foreseeable. Given that Defendant held vast amounts of Private Information, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the Private Information—whether by malware or otherwise.

105. Private Information is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the Private Information of Plaintiff and Class members' and the importance of exercising reasonable care in handling it.

106. Defendant improperly and inadequately safeguarded the Private Information of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

107. Defendant breached these duties as evidenced by the Data Breach.

108. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and Class members' Private Information by:

a. disclosing and providing access to this information to third parties and

b. failing to properly supervise both the way the Private Information was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

109. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal

information and Private Information of Plaintiff and Class members which actually and proximately caused the Data Breach and Plaintiff and Class members' injury.

110. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and Class members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff and Class members' injuries-in-fact.

111. Defendant has admitted that the Private Information of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

112. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and Class members have suffered or will suffer damages, including fraud, monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

113. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and Class members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their Private Information by criminals, improper disclosure of their Private Information, lost benefit of their bargain, lost value of their Private Information, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

SECOND CAUSE OF ACTION
Negligence *per se*
(On Behalf of Plaintiff and the Class)

114. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

115. Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class members' Private Information.

116. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted, and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect the Private Information entrusted to it. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff and the Class members' sensitive Private Information.

117. Defendant breached its respective duties to Plaintiff and Class members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Private Information.

118. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

119. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that,

because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

120. But for Defendant's wrongful and negligent breach of its duties owed, Plaintiff and Class members would not have been injured.

121. The injury and harm suffered by Plaintiff and Class members was the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their Private Information.

122. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

THIRD CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

123. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

124. Plaintiff and Class members were required to provide their Private Information to Defendant as a condition of receiving employment from Defendant. Plaintiff and Class members provided their Private Information to Defendant in exchange for Defendant's employment.

125. Plaintiff and Class members reasonably understood that a portion of the funds generated by their employment would be used to pay for adequate cybersecurity measures.

126. Plaintiff and Class members reasonably understood that Defendant would use adequate cybersecurity measures to protect the Private Information that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

127. Plaintiff and the Class members accepted Defendant's offers by disclosing their Private Information to Defendant in exchange for employment.

128. In turn, and through internal policies, Defendant agreed to protect and not disclose the Private Information to unauthorized persons.

129. In its Privacy Policy, Defendant represented that it had a legal duty to protect Plaintiff's and Class Member's Private Information.

130. Implicit in the parties' agreement was that Defendant would provide Plaintiff and Class members with prompt and adequate notice of all unauthorized access and/or theft of their Private Information.

131. After all, Plaintiff and Class members would not have entrusted their Private Information to Defendant in the absence of such an agreement with Defendant.

132. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

133. The covenant of good faith and fair dealing is an element of every contract. Thus, parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—and not merely the letter—of the bargain. In short, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

134. Subterfuge and evasion violate the duty of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or consist of inaction. And fair dealing may require more than honesty.

135. Defendant materially breached the contracts it entered with Plaintiff and Class members by:

a. failing to safeguard their information.

b. failing to notify them promptly of the intrusion into its computer systems that compromised such information.

c. failing to comply with industry standards.

d. failing to comply with the legal obligations necessarily incorporated into the agreements; and

e. failing to ensure the confidentiality and integrity of the electronic Private Information that Defendant created, received, maintained, and transmitted.

136. In these and other ways, Defendant violated its duty of good faith and fair dealing.

137. Defendant's material breaches were the direct and proximate cause of Plaintiff's and Class members' injuries (as detailed *supra*).

138. Plaintiff and Class members performed as required under the relevant agreements, or such performance was waived by Defendant's conduct.

FOURTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

139. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

140. Given the relationship between Defendant and Plaintiff and Class members, where Defendant became guardian of Plaintiff's and Class members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for Plaintiff and Class members, (1) for the safeguarding of Plaintiff and Class members' Private Information; (2) to timely notify Plaintiff and Class members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

141. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class members

upon matters within the scope of Defendant's relationship with them—especially to secure their Private Information.

142. Plaintiff and the Class were exclusively dependent on Defendant to implement adequate data security practices and had no control over the manner in which Defendant maintained or protected their Private Information.

143. Because of the highly sensitive nature of the Private Information, Plaintiff and Class members would not have entrusted Defendant, or anyone in Defendant's position, to retain their Private Information had they known the reality of Defendant's inadequate data security practices.

144. Defendant breached its fiduciary duties to Plaintiff and Class members by failing to sufficiently encrypt or otherwise protect Plaintiff's and Class members' Private Information.

145. Defendant also breached its fiduciary duties to Plaintiff and Class members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

146. Defendant understood the importance of protecting the data that it collected and the severe consequences that would result to Plaintiff and Class Members should it fail to implement reasonable safeguards.

147. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

FIFTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

148. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

149. This claim is pleaded in the alternative to the breach of implied contract claim.

150. Plaintiff and Class members conferred a benefit upon Defendant. After all, Defendant benefitted from (1) the revenues generated from Plaintiff and the Class's employment and (2) using their Private Information to provide employment and facilitate its business operations.

151. Defendant appreciated or had knowledge of the benefits it received from Plaintiff and Class members. And Defendant benefited from the revenue generated by Plaintiff and the Class's employment and from receiving Plaintiff's and Class members' Private Information, as this was used to provide employment and facilitate its business operations.

152. Plaintiff and Class members reasonably understood that Defendant would use adequate cybersecurity measures to protect the Private Information that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

153. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class members' Private Information.

154. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiff and Class members by utilizing cheaper, ineffective security measures. Plaintiff and Class members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

155. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and Class members' employment because Defendant failed to adequately protect their Private Information.

156. Plaintiff and Class members have no adequate remedy at law.

157. Defendant should be compelled to disgorge into a common fund—for the benefit of Plaintiff and Class members—all unlawful or inequitable proceeds that it received because of its misconduct.

PRAYER FOR RELIEF

Plaintiff and Class members respectfully request judgment against Defendant and that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing her counsel to represent the Class.

B. Awarding declaratory and other equitable relief as necessary to protect the interests of Plaintiff and the Class.

C. Awarding injunctive relief as necessary to protect the interests of Plaintiff and the Class.

D. Enjoining Defendant from further unfair and/or deceptive practices.

E. Awarding Plaintiff and the Class damages including applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law.

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial.

G. Awarding attorneys' fees and costs, as allowed by law.

H. Awarding prejudgment and post-judgment interest, as provided by law.

I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting other relief that this Court finds appropriate.

DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial for all claims so triable.

Dated: June 13, 2025

By: */s Casondra Turner* (MA BBO No. 687682)

MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
800 S. Gay Street, Suite 1100
Knoxville, TN 37929
Tel : (866) 252-0878
cturner@milberg.com

Samuel J. Strauss
Raina C. Borrelli
STRAUSS BORRELLI PLLC
One Magnificent Mile
980 N Michigan Avenue, Suite 1610
Chicago IL, 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
sam@straussborrelli.com
raina@straussborrelli.com

Attorneys for Plaintiff and the Proposed Class